Abstract

In a method for authorizing a transaction by a user with the aid of a terminal
(18) which can communicate with a background system (10), a secret, which

5   is known to the user and to the background system (10) but not to an
unauthorized attacker, is used. The background system (10) transmits secret
data, which indicate the secret, only to the terminal (18) if the terminal (18)
has successfully authenticated itself at the background system (10). Because,
as a rule, secret data of several users are stored in the background system

10   (10), the terminal (18) detects in advance identification information which
identifies the user, and transmits corresponding user identification data to
the background system (10). When the terminal (18) displays the secret to the
user, the user can be certain that the terminal (18) is trustworthy. A device
and a computer program product comprise corresponding features. The

15   invention provides a technique for authorizing a transaction by a user with
the aid of a terminal (18) which enables the user to recognize a falsified
terminal (18).

(Fig. 1)